POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Dezembro de 2024

1. PRINCÍPIOS

Esta Política de Segurança da Informação e Segurança Cibernética especifica os controles internos aplicáveis à segurança e ao sigilo da informação das sociedades que fazem parte do Conglomerado FIDD, FIDD Administração de Recursos Ltda. e FIDD Distribuidora de Títulos e Valores Mobiliários Ltda. ("Grupo FIDD" ou "FIDD"), com o objetivo de prover a segurança necessária para realização de suas operações, ainda que em situações adversas.

A presente política é compatível com o porte, o perfil de risco e o modelo de negócios da FIDD, com a natureza de suas operações e a complexidade dos seus produtos, serviços, atividades, processos e da sensibilidade dos dados e das informações sob sua responsabilidade.

2. ABRANGÊNCIA

Esta política deve ser observada por todos os colaboradores, acionistas, administradores, prestadores de serviços ou parceiros de negócios da FIDD, que devem ser diligentes na condução de atividades.

3. NORMAS DE REFERÊNCIA

- Resolução BCB n° 85 de 8 de abril de 2021;
- Guia de Cibersegurança ANBIMA;
- Lei n° 13.709 - Lei Geral de Proteção de Dados Pessoais, de 14 de agosto de 2018.

4. DEFINIÇÕES

Para os efeitos desta Política, entende-se por:

Antivírus: programa que detecta e elimina vírus de computador.

Ativos: ativos de informação, ativos de software e ativos físicos.

Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

Ativos físicos: equipamentos computacionais (computadores, processadores, monitores, laptops, modens, etc.), equipamentos de comunicação (roteadores, PABX, telefones fixos, etc.), mídias (fitas e discos magnéticos, discos ópticos, etc.), outros equipamentos técnicos (nobreaks, aparelhos de ar-condicionado, etc.), mobília, acomodações, etc.

Ativos de informação: base de dados e arquivos, documentação de sistemas, políticas ou regimentos ou normativos ou manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade de negócio, procedimentos de recuperação, informações armazenadas, etc.

Backup: cópia exata de um programa, disco ou arquivo de dados feito para fins de arquivamento ou para salvaguardar informações.

Colaboradores: são as pessoas naturais ou jurídicas contratadas pela FIDD para desenvolvimento de suas atividades na forma do seu contrato social. São considerados

colaboradores os funcionários, estagiários, menores aprendizes, sócios e diretores bem como terceiros contratados que atuem internamente e/ou de forma exclusiva para a FIDD.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Controle de acesso: conjunto de restrições ao acesso às informações de um sistema exercido pela equipe de segurança da informação.

Criptografia: arte/ciência de utilizar matemática para tornar a informação segura, criando um grande nível de confiança no meio eletrônico.

Dados Pessoais: se refere a qualquer informação relativa a uma pessoa física identificada ou identificável, que pode ser identificada, direta ou indiretamente.

Direito de Acesso: privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Download: transferência de arquivo de um computador remoto para outro computador através da rede.

Ferramentas: conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades.

Gestor da informação: colaboradores ou áreas da FIDD, no exercício de suas competências, produz ou obtém e guarda, seja de fonte externa ou interna, informações de propriedade de pessoa física ou jurídica, dentro de seus servidores de arquivos ou banco de dados;

Incidente em segurança da informação: qualquer indício de fraude, sabotagem, desvio, falha, tentativa ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações ou ameaçar a segurança da informação.

Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

Incidente de Segurança: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Junk mail: e-mails não solicitados por usuários não interessados em recebê-los.

Log: registro das transações ou atividades realizadas em sistema de computador.

Peer-to-Peer: rede por meio da qual usuários compartilham entre si seus recursos, possibilitando a provisão de conteúdo e serviços à rede.

Política de Segurança: conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos sistemas de informação.

Proteção dos Ativos: processo pelo qual os ativos devem receber classificação quanto ao respectivo grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém.

Segurança da informação: proteção da informação contra ameaças para garantir sua continuidade, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio.

Spam: e-mail não solicitado enviado a grande número de endereços eletrônicos, que geralmente visam fazer propaganda de produtos e serviços.

Vírus: programa construído para causar danos aos softwares do computador.

Cavalo de Tróia (Trojan Horse): programa que pode danificar áreas da máquina e torná-la vulnerável ao ataque de hackers.

5. DIRETRIZES

5.1. Objetivos

Esta Política tem como objetivos:

(i) Permitir que a FIDD atenda à regulamentação, legislação e autorregulação aplicáveis;
(ii) Manter o nível de segurança da organização em um patamar definido como adequado pela FIDD;
(iii) Garantir que as diretrizes explicitadas nesta Política sejam praticadas, por meio da implementação de controles que visam garantir a confidencialidade, a integridade e a disponibilidade das informações.

Para atingir os objetivos acima listados, a FIDD estabelece a presente Política como um dos pilares de sua estratégia de segurança, que deve ser seguida e implementada para garantir que os Ativos sejam protegidos de acordo com a sua importância estratégica para a organização.

A presente Política se define como um documento que expressa a posição da organização sobre a segurança, quais são seus valores e direcionamentos para minimizar os riscos sobre seus Ativos. Desta forma ela estabelece a linha mestra de atuação da FIDD em relação a todos os aspectos da segurança da informação, incluindo equipamentos, bens, informações e pessoas.

5.2. Princípios

A Política tem como princípios assegurar a:

(i) Identificação: garantir que qualquer indivíduo seja identificado unívoca e inequivocamente;

(ii) Autenticação: garantir que a identidade de cada pessoa ou recurso seja expressamente comprovada;

(iii) Autorização: garantir que somente as pessoas e recursos permitidos tenham acesso aos Ativos;

(iv) Confidencialidade: garantir que as informações sejam acessadas apenas por aqueles que possuam esse acesso como pré-requisito para o exercício de suas funções ou que sejam expressamente autorizados;

(v) Integridade: preservar a integridade das informações, salvaguardando-as contra ações não autorizadas e garantindo que todas as informações estejam exatas e completas durante a sua criação, uso, guarda e destruição;

(vi) Disponibilidade: garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

6. DEVERES E RESPONSABILIDADES

São deveres de todos os Colaboradores no âmbito desta Política:

(i) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

(ii) Cumprir a presente Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

(iii) Utilizar os sistemas de informações e os recursos relacionados somente para atividades necessárias cumprimento das atividades de negócios;

(iv) Cumprir as regras específicas de proteção estabelecidas aos Ativos de informação;

(v) Manter o caráter sigiloso de senhas de acesso aos recursos e sistemas, sem compartilhar acessos ou permitir usos por outras pessoas (“caronas”);

(vi) Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;

(vii) Responder por todo e qualquer acesso aos recursos da FIDD, bem como pelos efeitos decorrentes de acesso efetivado através de seu código de identificação, ou outro atributo para esse fim utilizado;

(viii) Solicitar acesso a informações restritas somente quando houver real necessidade de acessar o recurso;

(ix) Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, sob pena de violação da legislação de propriedade intelectual pertinente; e

Comunicar ao seu superior imediato e à Diretoria de Riscos e Equipe de Segurança da Informação o conhecimento de qualquer irregularidade ou desvio verificado no âmbito da presente Política, com a garantia que sua comunicação será tratada de modo sigiloso e sem identificação pública de que foi feita.

6.1. Responsabilidades dos Gestores de Áreas

(i) Gerenciar o cumprimento desta Política, por parte de seus funcionários e prestadores de serviço;

(ii) Identificar os desvios praticados e adotar as medidas corretivas apropriadas, reportando a situação à Diretoria de Riscos e Equipe de Segurança da Informação;

(iii) Fornecer à Equipe de Segurança da Informação informações sobre movimentação de funcionários em sua equipe (desligamento, contratação, transferência etc.) para que os responsáveis promovam a criação, modificação ou cancelamento da respectiva permissão de acesso;

(iv) Proteger os ativos de informação e de processamento da FIDD;

(v) Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger todos os ativos de informação da FIDD;

(vi) Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de tecnologia da informação quais são os empregados e prestadores de serviço, sob sua supervisão, que podem acessar as informações da FIDD; e

(vii) Comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de tecnologia da informação, quais são os empregados demitidos ou transferidos, para que esta possa prosseguir com as respectivas exclusões no cadastro de usuários.

6.2. Responsabilidades da Equipe de Segurança da Informação

(i) Estabelecer as regras de proteção dos Ativos da FIDD;

(ii) Revisar frequentemente as regras de proteção estabelecidas;

(iii) Restringir e controlar o acesso e privilégios de usuários remotos e externos;

(iv) Auxiliar as demais Diretorias da FIDD a elaborar e a manter atualizado o Plano de Contingência e Continuidade dos Negócios;

(v) Executar as regras de proteção estabelecidas por esta Política;

(vi) Detectar, identificar, registrar e comunicar à chefia violações ou tentativas de acesso não autorizadas;

(vii) Definir e aplicar, para cada usuário de tecnologia da informação, restrições de acesso à rede, como horário e dia autorizados, entre outras;

(viii) Limitar ao período da contratação o prazo de validade das contas de prestadores de serviço;

(ix) Solicitar e gerir, quando necessário, auditoria para verificação de acessos indevidos;

(x) Solicitar, quando julgar necessário, o bloqueio de chaves de acesso de usuários;

(xi) Excluir ou desabilitar as contas inativas;

(xii) Fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;

(xiii) Garantir o cumprimento do procedimento de backup para os servidores e Ativos; e

(xiv) Controlar os acessos dos colaboradores da FIDD, inclusive quanto ao acesso às portas de transferência de dados, criando os perfis de acesso e designando-os a cada Colaborador de acordo com as atividades por ele desenvolvidas e com o cargo por ele ocupado;

(xv) Atualizar a política de perfis e acessos, bem como executar a liberação ou o bloqueio de perfis de acordo com as necessidades verificadas ou sob demanda dos Colaboradores quando julgar pertinente;

(xvi) Aprovar a criação ou exclusão de usuários por solicitação do RH, quando houver contratação ou demissão de Colaboradores, sendo certo que os usuários novos devem ser cadastrados sem nenhum acesso, os quais devem ser solicitados posteriormente pela sua Gerência; e

(xvii) Organizar treinamentos obrigatórios relacionados à segurança dos Ativos de informação anualmente, com a finalidade de capacitar e avaliar os Colaboradores.

6.3. Responsabilidades da Diretoria de *Compliance*

(i) Assessorar a FIDD na elaboração e verificação da conformidade dos regulamentos, termos, políticas e controles utilizados para proteger os Ativos de informação;

(ii) Junto com a Diretoria de Riscos e Equipe de Segurança da Informação, acompanhar o processo de apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de segurança da informação aos regulamentos internos e externos da FIDD;

(iii) Assegurar que as atividades da FIDD sejam desenvolvidas com base nos princípios estabelecidos em seus manuais/políticas internos e em consonância com a regulamentação, legislação e autorregulação aplicável;

(iv) Dirimir ou mitigar ao máximo a existência de conflitos de interesse relacionados ao desenvolvimento das atividades da FIDD, especialmente, para fins do disposto nesta Política;

(v) Acompanhar a segregação física e lógica entre as atividades que necessitarem de segregação nos termos da regulamentação em vigor ou pelo nível de confidencialidade das informações que forem conduzidas por tais áreas, por meio da restrição de acessos e da criação de perfis de usuários para a rede interna.

6.4. Responsabilidades da Gerência Jurídica

(i) Assessorar a Diretoria de Riscos e Equipe de Segurança da Informação na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os ativos de informação;

(ii) Garantir junto à Diretoria de Riscos, que os contratos celebrados com terceiros, sempre que necessário, contenham cláusula de confidencialidade e que preserve a segurança das informações e proteção de dados da FIDD; e

(iii) Garantir que a existência das diretrizes estabelecidas com base nesta Política e a necessidade do cumprimento de suas premissas sejam referenciadas nos contratos e acordos

com terceiros, bem como nos contratos firmados com os Colaboradores da FIDD, de forma que cada um saiba suas obrigações, direitos e deveres no âmbito desta Política.

6.5. Responsabilidades Administrativas da Diretoria de Riscos e Equipe de Segurança da Informação

(i) Executar as atividades de administração dos meios de informação não informatizados da organização, tais como: copiadoras, telefonia, controle de acesso físico, arquivo, correio, mensageiros, impressoras, cabeamento, fragmentadores, entre outros;

(ii) Distribuir as funções específicas de segurança dos Ativos de informação entre os integrantes de sua equipe;

(iii) Classificar os meios de informação não computadorizados que administra quanto à criticidade que representam, provendo as condições mínimas necessárias de continuidade, disponibilidade, integridade e legalidade desses meios, incluindo locais, serviços e equipamentos;

(iv) Executar as ações para proteger os ativos de informação sob sua responsabilidade;

(v) Administrar os serviços de proteção, limpeza, transporte, armazenamento e destruição dos ativos de informação;

(vi) Assessorar a Equipe de TI, na criação, alteração e manutenção de novas políticas, normas, códigos ou regulamentos de segurança da informação;

(vii) Participar, quando cabível, na apuração das responsabilidades e causas relacionadas a incidentes ou violações da segurança da informação.

6.6. Responsabilidades dos Prestadores de Serviço

(i) Respeitar as obrigações previstas nos respectivos contratos de prestação de serviço, especialmente, para fins dessa Política, no que concerne à segurança da informação.

7. GESTÃO DA INFORMAÇÃO

7.1. Classificação da Informação

As informações, sejam itens, dados, conjuntos ou documentos que circulam ou são produzidas pela FIDD são confidenciais por definição, salvo disposição interna ou regulação ou legislação que obrigue sua divulgação. Todo Colaborador deve zelar pela manutenção de níveis de confidencialidade adequados, e sempre que possível tornar a classificação adotada de maneira explícita, seja no desenho dos processos ou fluxos de informação, seja no próprio documento ou documentação daquele conjunto de informações. Todas as informações obtidas ou geradas pela FIDD e terceiros são classificadas nos seguintes níveis:

(i) Confidencial: É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para

trazer grandes prejuízos financeiros ou à imagem da FIDD. São protegidas por rigorosos controles de acesso e criptografia.

(ii) Restrita: É o nível intermediário de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de Colaboradores. São protegidas por controle de acesso à módulos de sistemas e/ou diretórios em nuvem.

(iii) Uso interno: Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

(iv) Pública: São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público.

Abaixo uma tabela, não exaustiva, que lista alguns itens de informação em cada categoria:

Categoria de Classificação	Exemplos de itens, conjuntos ou elementos de informação
Confidencial	Planos de negócio, Documentos de apreciação para Diretoria Colegiada, memorandos ou atas de reuniões restritas à Diretoria Colegiada, dados de Remuneração e Pessoais dos Colaboradores e Diretores, Documentos resultantes de Auditorias internas e externas, Documentos restritos de reguladores. Resultados de *Background Check* feito sobre Colaboradores, cotistas e outros prestadores de serviço.
Restrita	Estratégias de negócio ou de marketing, Documentos de Fundos de Investimento sobre operações a serem realizadas ou em realização, documentos e dados pessoais de cotistas, documentos e dados pessoais de Colaboradores.
Uso Interno	Apresentações internas das mais diversas, trocas de informações entre áreas, materiais de divulgação interna, políticas e manuais não públicos, documentos e dados de processos internos.
Pública	Apresentações institucionais, materiais de divulgação, textos de blog, documentos relativos à fundos que devem estar disponibilizados em sites públicos ou de forma pública nos sites da FIDD

7.2. Manutenção do Sigilo da Informações

As seguintes regras devem ser observadas por todos os Colaboradores quando da utilização de informações confidenciais e/ou restritas:

(i) Os Colaboradores devem proteger a confidencialidade de quaisquer informações obtidas durante o exercício de suas funções na FIDD, que não devem ser (1) divulgadas a terceiros, (2) divulgadas ou disponibilizadas em domínio público, (3) copiadas ou transferidas (mesmo que por foto) a celulares, tablets, computadores pessoais ou quaisquer outros

dispositivos portáteis e/ou (4) enviadas para correio eletrônico (e-mails) externos, ainda que pertencentes ao próprio Colaborador;

(ii) A obrigação de sigilo prevista no item anterior, se aplica mesmo após a rescisão do vínculo do Colaborador da FIDD, qualquer que seja a razão, permanecendo o Colaborador obrigado a manter sigilo e a proteger a confidencialidade das informações obtidas durante o exercício de suas funções na FIDD;

(iii) Os Colaboradores respondem individualmente, civil e criminalmente, pela divulgação indevida de Informações Confidenciais ou pela divulgação de quaisquer informações que tenham por objetivo atingir a honra ou a imagem da FIDD ou dissuadir seu relacionamento com clientes.

(iv) Questões envolvendo informações confidenciais e restritas de titularidade da FIDD não devem ser discutidas pelos Colaboradores em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes, etc.

(v) Os programas de correio eletrônico (e-mails) disponibilizados pela FIDD às pessoas autorizadas devem ser utilizados exclusivamente para mensagens de âmbito profissional e não podem, em hipótese alguma, ser usados para transmitir ou retransmitir mensagens ou seus anexos de qualquer natureza e conteúdo que possam comprometer a FIDD.

(vi) A FIDD adota a política de mesa limpa. Todos os Colaboradores devem evitar manter papéis e documentos confidenciais expostos em suas mesas de trabalho. Documentos confidenciais devem ser guardados em local apropriado e com chave, mesmo no decorrer do expediente, para evitar o acesso de terceiros não autorizados. Ao final do expediente, os armários devem permanecer trancados e as mesas sem papéis ou documentos.

(vii) As informações confidenciais de clientes enviadas ou entregues à FIDD para execução de transações são protegidas por lei. O compartilhamento destas informações com terceiros depende de expressa autorização dos clientes, por escrito.

(viii) Nas operações passivas da FIDD, em especial quando se tratar de distribuição de cotas de fundos a clientes, quando aplicável, os Colaboradores devem firmar documentos específicos com os distribuidores dos fundos sob administração ou gestão, com dispositivos específicos prevendo:

a. A obrigação de os distribuidores adotarem política de privacidade e confidencialidade de dados dos clientes;

b. A garantia aos clientes da devida observância destas políticas pelo distribuidor e pelas pessoas a ele vinculadas;

c. Minimização de riscos de imagem para a FIDD, evitando que clientes vinculem a FIDD a uma eventual falha do distribuidor na proteção das Informações Confidenciais.

(ix) A FIDD poderá revelar as informações confidenciais e restritas nas seguintes hipóteses:

a. Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;

b. Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela FIDD a defender seus direitos e créditos;

c. Aos órgãos reguladores do mercado financeiro; e

d. Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

7.3. Utilização de Conteúdo Protegido por Direitos Autorais

A maioria das informações e softwares que estão disponíveis em domínio público (incluindo a internet) está protegida por leis de Propriedade Intelectual, portanto:

(i) Não é permitido obter softwares, mídias e outros conteúdos destas fontes, exceto quando houver permissão explícita por parte do respectivo proprietário e autorização pela Equipe de Segurança da Informação da FIDD;

(ii) Deve-se ler e compreender todas as restrições dos direitos autorais do conteúdo e, caso a FIDD não possa cumprir com as condições estipuladas, não faça download e não utilize o respectivo material;

(iii) É proibido o uso de qualquer foto, imagem ou desenho que possua marca registrada de terceiros. Podem ser utilizadas imagens originais do Sistema Operacional ou imagens não relacionadas a Produtos, Empresas ou Pessoas. Imagens consideradas agressivas também não devem ser utilizadas;

(iv) Em caso de dúvidas em relação às licenças ou a qualquer dos pontos acima, o Colaborador deve entrar em contato com a Diretorias de Riscos e Equipe de Segurança da Informação.

7.4. Outras orientações para prevenção do vazamento de dados

Além disso, a FIDD orienta seus colaboradores com os seguintes itens para prevenir o vazamento de dados:

(i) manter os documentos de pessoas físicas e jurídicas, sejam eles CPF, RG, CNH, comprovante de residência, documentação societárias, entre outros, armazenados em pastas específicas, segregadas, com acessos limitados e controlados;

(i) revisão periódica dos arquivos que estão no computador para eliminar documentos que foram digitalizados dos clientes, fornecedor ou qualquer colaborador ou empresa;

(ii) não compartilhar arquivos que contenham dados pessoais para terceiros estranhos à atividade, sem autorização prévia;

(iii) verificar arquivos digitais que contenham dados pessoais dos clientes armazenados em planilhas e eliminando-os. Caso haja necessidade de compartilhamento, comunicar o gestor e diretor da área responsável;

(iv) não utilizar rascunhos que contenham dados pessoais;

(v) no descarte seguro de documentos físicos, rasgue e picote antes de jogar no lixo;

(vi) no descarte seguro de documentos digitais, caso esteja em um dispositivo que permaneça sob propriedade da FIDD, conferir e excluir o documento da lixeira eletrônica, caso exista esse serviço. Caso o dispositivo seja descartado ou repassado para um terceiro, acionar a equipe de TI para realizar a limpeza segura do dispositivo;

(vii) sempre que um colaborador for remanejado para outra área ou unidade, os acessos de sistemas devem ser revisados;

(viii) antes de compartilhar qualquer informação em uma reunião virtual ou física, mesmo que verbalmente, certificar-se de que todos os membros podem ter acesso àquela informação.

Além disso, os equipamentos antigos poderão ser doados após passarem por um procedimento de limpeza segura. Os mesmos deverão ser direcionados à equipe de TI, que realizará a formatação adequada dos dispositivos, de modo a impossibilitar a recuperação de qualquer dado.

8. ORIENTAÇÕES DE SEGURANÇA

8.1. Privacidade

A FIDD tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede ou "nuvem", que se encontrem fisicamente no mobiliário do escritório, como, por exemplo, em mesas, estantes, gaveteiros, armários etc. Dessa forma, ainda que o Colaborador possa se utilizar da estrutura de tecnologia da organização para algum uso particular não conflitante, tais informações podem ser acessadas pela FIDD mesmo sem o prévio consentimento do respectivo Colaborador.

Com relação às ligações telefônicas, e-mails e outros canais de comunicação internos, a FIDD se reserva o direito de monitorar e armazenar registros das ligações e conversas de texto, bem como consultá-las sem prévio aviso ao Colaborador.

Sem prejuízo do acima exposto, a FIDD garante que toda escuta a conversas telefônicas e mensagens de texto depende do prévio consentimento da Diretoria de Riscos. Mais ainda, a FIDD se compromete a zelar pelo sigilo de qualquer informação, incluindo de caráter pessoal, que eventualmente se depare nos processos de monitoramento.

A FIDD orienta que todo e qualquer evento considerado como violação de privacidade, seja reportado nos canais oficiais e registrado no Sistema de Compliance da organização. Todos os colaboradores devem observar outros documentos correlatos, tais como a Política de Privacidade e Proteção de Dados Pessoais.

8.2. Proteção de Dados Pessoais

Com relação ao titular dos dados que navegam no site com ou sem cadastro, a FIDD poderá coletar informações como as seguintes: endereço de Protocolo de Internet (endereço IP), registro de acesso, geolocalização do endereço IP, tipo do navegador utilizado, versão do sistema operacional, modelo e características do aparelho móvel, banda de internet,

operadora, comportamento de pageview e páginas visitadas. No cadastro, o titular do dado poderá fornecer diversos dados, incluindo informações pessoais identificáveis, tais como: nome completo, número do CPF, número e tipo do documento de identidade (RG, RNE, CNH), data de nascimento, sexo, estado civil, nome do cônjuge, e-mail, telefone, endereço residencial, cep, profissão, renda, patrimônio, informações sobre vínculo com pessoa politicamente exposta, informações sobre vínculo com a FIDD, senha de acesso. Além disso, o titular do dado fornecerá informações bancárias, como banco, número da agência e da conta corrente.

O titular do dado poderá também oferecer dados pessoais, incluindo via webAPI, fotografias de documentos ou documentos digitalizados, tais como documentos de identidade (RG, RNE, CNH), foto do comprovante de residência e documentos que comprovem a existência de conta conjunta (cópia do cartão, do cheque ou declaração do banco).

A coleta de dados pessoais referentes à geolocalização poderá ocorrer em aplicativos, caso tal opção esteja ativa e seu uso seja autorizado pelo titular do dado, e na página da FIDD por meio da região do endereço IP de acesso. A finalidade da coleta de tais informações é primariamente a identificação de bugs, lentidão e monitoramento.

O titular do dado entende que a FIDD pode coletar informações (incluindo dados pessoais) a respeito do titular do dado de fontes externas, bureaus de créditos e de dados, para complementar o cadastro e detectar possíveis fraudes, exclusivamente para fins de cumprimento de obrigação legal/ regulatória.

A titularidade do cadastro é pessoal. Apenas o titular da conta pode ter acesso aos dados pessoais a ela relativos. Alterações em dados cadastrais somente podem ser feitas pelo próprio titular do dado em sua conta. A FIDD não tem prerrogativa para fazer esse tipo de alteração unilateralmente.

Caso a FIDD identifique inconsistências ou eventuais riscos em relação ao titular do dado ou às suas atividades, que considere necessário validar informações envolvendo os dados pessoais, o titular se compromete a fornecer as informações, documentos e demais comprovações que lhe forem requisitadas.

Havendo motivos que indiquem que os dados cadastrados (inclusive os dados pessoais) não são verdadeiros ou demonstre qualquer suspeita de fraude, a FIDD tem o direito de suspender ou encerrar o relacionamento, bem como de recusar a prover quaisquer dos serviços. Qualquer erro, atraso, prejuízo ou dano causado devido ao cadastramento de dados (inclusive dados pessoais) incorretos, incompletos ou desatualizados é de total responsabilidade do titular do dado.

8.3. Proteção do Patrimônio Físico e Intangível

Integram o patrimônio físico e intangível da FIDD, seus imóveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos funcionários, não podendo os mesmos serem utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, independentemente do fim.

Não podem ser utilizados equipamentos ou outros recursos da FIDD para fins particulares, salvo se previamente autorizado pelo gestor de área, sendo a referida aprovação vetada nos casos em que interfira no seu trabalho, ou se ainda:

(i) Interferir ou concorrer com os negócios da FIDD;

(ii) Fornecer informações a terceiros;

(iii) Envolver solicitação comercial ou outra solicitação não apropriada ao negócio, e;

(iv) Envolver custo adicional para a FIDD.

8.4. Uso do E-mail

O uso do e-mail na FIDD está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. O e-mail não deve substituir uma conversar presencial ou um telefonema, quando este for mais eficiente. Mas pode e deve ser usado como documento de comunicação, interno e externo. Com isso em vista, seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização desta ferramenta:

(i) O usuário é o único responsável pelo conteúdo das transmissões feitas através do e-mail a partir de sua conta e senha;

(ii) O uso da conta de e-mail corporativo da FIDD é para fins profissionais, sendo permitido seu uso pessoal com bom-senso, para assuntos que não sejam conflitantes com as atividades da FIDD nem que prejudiquem qualquer lei, regulação ou regulamento e políticas internas da FIDD.

(iii) As mensagens de e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela;

(iv) Não devem ser abertos arquivos ou executados programas anexados aos e-mails sem antes ter certeza de sua procedência e existência de prévia expectativa do recebimento da mensagem;

(v) Não deve ser utilizado e-mail para fins ilegais;

(vi) Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço;

(vii) Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual;

(viii) Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis;

(ix) O Colaborador não pode obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço;

(x) Não devem ser utilizados os serviços de e-mail para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia" ou outro programa prejudicial;

(xi) Não devem ser transmitidas mensagens não-solicitadas, conhecidas como *spam* ou *junk mail*, correntes, *chain letters* ou distribuição em massa de mensagens não-solicitadas, salvo mensagens informativas de produtos e serviços da FIDD, aprovada por um Diretor, por lista controlada e via ferramentas oficiais contratadas pela FIDD. Quando este envio ocorrer, deve contar com sistema de cancelamento de cadastramento na própria mensagem;

(xii) Mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por outros usuários, sem que se esteja cuidando para retirar a impressão antes do acesso físico ao conteúdo impresso, de forma inadvertida, pelos demais usuários;

(xiii) O e-mail deve estar ativo sempre que o usuário estiver trabalhando no microcomputador. Quando este se afastar de sua estação de trabalho, deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal;

(xiv) É proibido aos administradores de rede ou e-mail ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte, salvo por necessidade de apuração de eventos que tenham causado danos, ou tenham sido classificados como potencialmente danosos à FIDD ou a terceiros ou por determinações da Diretoria de *Compliance*, desde que devidamente justificado, ou, ainda, de Reguladores ou Autoridades para apuração de eventos de infração de alguma regulação ou legislação; e

(xv) Não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura de rede local ou que violem as leis de direitos autorais.

8.5. Uso do Telefone Fixo

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização destas ferramentas:

(i) O uso do telefone fixo na FIDD deve ter uso para fins profissionais. É permitido o uso para fins pessoais com bom-senso, para assuntos que não sejam conflitantes com as atividades da FIDD nem que prejudiquem qualquer lei, regulação ou regulamento e políticas internas da FIDD. Vale lembrar também que todas as ligações são gravadas e podem ser ouvidas pela FIDD como determinam suas políticas.

(ii) O uso de telefone localizado fora das dependências da FIDD para discussão de assuntos confidenciais internos pode ser necessário, principalmente em situações de contingência, porém pode gerar exposição de segurança, portanto, deve-se sempre priorizar fazer ligações dentro da FIDD, ou pelos meios eletrônicos de telefonia e comunicação disponibilizados pela empresa via computador e/ou aplicativos aprovados pela Equipe de Segurança da Informação. Caso não seja possível, deve-se certificar que não existem terceiros ouvindo a ligação;

(iii) Não se deve deixar mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas; e

(iv) Ao coordenar uma teleconferência ou videoconferência, deve-se garantir que todos os participantes foram devidamente autorizados antes de começar a reunião.

8.6. Uso da Internet

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização da internet em dispositivos da organização ou na utilização de dispositivos pessoais na rede corporativa da FIDD:

(i) Alguns sites (páginas da internet) contêm ou distribuem material não apropriado ao ambiente de trabalho, portanto, os Colaboradores não devem acessar tais sites nem tampouco distribuir / obter material similar;

(ii) Os acessos a sites podem estar sendo monitorados a qualquer tempo, portanto, em caso de dúvida, deve-se verificar junto aos superiores imediatos ou o time de SI se o respectivo site pode ser acessado;

(iii) É permitido o uso de serviços de mensagens ou chat (WhatsApp, Hangouts, etc.) desde que para fins profissionais. O uso pessoal desses aplicativos deve ser limitado e com bom-senso, nunca com finalidades conflitantes com os interesses da FIDD, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas da FIDD. Vale lembrar também que todas as comunicações feitas em computadores da FIDD ficam armazenadas e podem ser consultadas pela FIDD como determinam suas políticas, bem como o compartilhamento de qualquer assunto referente à FIDD é expressamente proibido, sendo apenas autorizado com expressa comunicação da Diretoria de *Compliance*;

(iv) É permitido o acesso a redes sociais (Facebook, LinkedIn, Instagram, X), desde que com bom-senso, nunca com finalidades conflitantes com os interesses da FIDD, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas da FIDD. Vale lembrar também que todas as comunicações feitas em computadores da FIDD ficam armazenadas e podem ser consultadas pela FIDD como determinam suas políticas. Vale lembrar que o compartilhamento de qualquer assunto referente à FIDD é expressamente proibido, sendo apenas autorizado com expressa comunicação da Diretoria de *Compliance;*

(v) O acesso a e-mails não corporativos nos computares de propriedade da FIDD é vetado, sendo proibido o acesso por qualquer meio inclusive via Webmail, exceto nos casos em que para viabilizar o uso de alguma ferramenta ou aplicativo autorizado pela Diretoria de Riscos e Equipe de Segurança da Informação, seja necessário o acesso a alguma conta de e-mail pessoal;

(vi) Não é permitido o uso de compartilhadores de informações como redes peer-to-peer, também conhecidas como redes P2P dentro das dependências da FIDD;

(vii) Não é permitido o download de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais;

(viii) É permitida a utilização de programas de *Streaming* de áudio nos computadores da FIDD, desde que com bom-senso, respeitando e priorizando o uso da infraestrutura de rede para fins profissionais e desde que sejam acessos lícitos e individualizados. Não são permitidos uso de programas de Streaming de vídeo, somente com aprovação expressa e limitada (tipo, tempo etc.) pela Diretoria de Riscos e Equipe de Segurança da Informação.

8.7. Uso das Impressoras

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização deste equipamento:

(i) Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;

(ii) Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;

(iii) As impressoras são ferramentas para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pela FIDD. Impressões para finalidade pessoal devem ser limitadas e com bom-senso, nunca com finalidades conflitantes com os interesses da FIDD, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas da FIDD.

8.8. Mesa Limpa

A política de mesa limpa consiste em não deixar informações confidenciais ou bens da FIDD, incluindo, mas não se limitando a papéis, pen-drives ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o funcionário estiver fora de sua estação de trabalho.

Ao final do dia de trabalho, computadores portáteis devem ser devidamente trancados em gaveta ou armário, ou serem presos a cabos de segurança ou levados pelo seu responsável, conforme estabelecido pelo respectivo gestor.

8.9. Tela Limpa

Computadores, notebooks e outros dispositivos devem estar protegidos por senha quando não estiverem sendo utilizados. Todos os computadores devem ter proteção de tela automática com senha habilitada para acionamento no tempo máximo de 5 minutos de inativação.

8.10. Senhas

A FIDD adota política de troca obrigatória de senhas com período de uso contínuo de no máximo 60 (sessenta) dias.

A senha é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do Colaborador, portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

(i) Manter sua confidencialidade;

(ii) Criar senhas fortes, respeitando, ao menos, os critérios abaixo:

a. As senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário); e

b. Devem ter pelo menos 8 caracteres, com ao menos um caractere especial e um número.

Os acessos, validados por meio da utilização de senha, serão limitados aos recursos e serviços necessários para o desempenho das atividades exercidas por cada Colaborador, e poderão ser revogados rapidamente quando necessário.

9. GESTÃO DA SEGURANÇA CIBERNÉTICA

9.1. Autenticação e Controle de Acesso

A prática de Controle de Acesso tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo assim a confidencialidade das informações.

Para garantir um nível aceitável de controle de acessos, são executados os seguintes processos:

(i) Controle de acessos através da matriz de segregação de função. Na matriz estão listadas todas as equipes, colaboradores e acessos liberados;

(ii) Execução de procedimentos formalizados para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo que para todos os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a matriz de segregação de função;

(iii) Todos os usuários são orientados a possuírem acesso apenas à informação de acordo com as necessidades de negócio;

(iv) É de responsabilidade do gestor da equipe o informe do nível de acessos para novos Colaboradores. Os acessos são limitados aos ativos de informação sob domínio da equipe do gestor.

(v) Todos os procedimentos de concessão e Alteração do Acesso dentro de uma equipe são aprovados pelo gestor responsável e executados pela Equipe de Segurança da Informação;

(vi) Existem casos específicos de colaboradores que necessitam de acesso aos ativos de informação pertencentes à outras equipes. Para estes casos, todos os procedimentos de Concessão e Alteração são aprovados pelo gestor responsável da equipe do colaborador e responsável pelo sistema;

(vii) A FIDD realiza revisão de acessos, no mínimo anualmente, conforme política, que tem como objetivo a atualização dos acessos e permissões, procedimento este, que é coordenado pela Equipe de Segurança da Informação, sendo o resultado da revisão enviado para a anuência do Subcomitê de Segurança da Informação;

(viii) O Controle de Acesso seguro, se aplica em situações de contingência e Continuidade de Negócios.

9.1.1. Serviços de diretório

Serviços de diretório desempenham um papel importante no desenvolvimento de aplicações intranet e Internet permitindo o compartilhamento de informações sobre usuários, sistemas, redes, serviços e aplicações através da rede.

A FIDD utiliza 2 (dois) serviços de diretório em paralelo: um para o acesso interno aos equipamentos dos Colaboradores e infraestrutura do escritório e outro para acesso aos serviços em nuvem. Os diretórios possuem sincronização ativa, logo, compartilham dos mesmos usuários, grupos, senhas e demais informações.

Sempre que possível os sistemas adquiridos e desenvolvidos possuem login integrado com o serviço de diretório em nuvem da FIDD, mantendo assim um canal único e centralizado de gestão de acessos.

9.1.2. Gerenciamento de Senhas e Acessos

Para alguns colaboradores e áreas críticas, a FIDD disponibiliza um serviço de cofre seguro, que é o meio ideal para armazenar e gerenciar informações confidenciais compartilhadas, como senhas, documentos e identidades digitais. O serviço é acessível apenas na rede interna do escritório ou via Rede virtual privada (VPN).

A ferramenta fornece controles de segurança preventiva e de investigação, através de fluxos para rotinas de aprovação e alertas em tempo real sobre senhas de acesso.

9.2. Controle Contra Software Malicioso

Os *malwares* de computador são programas desenhados para causar perda ou alteração de dados do computador, com isso em vista, todo equipamento da FIDD deve ter um programa antivírus instalado. Os softwares antivírus devem ser atualizados diariamente e de forma automática.

O Colaborador, ao receber alerta de vírus de qualquer fonte que não seja o antivírus, não deve acessá-lo ou encaminhá-lo a outras pessoas, pois geralmente estes alertas são falsos. De toda forma, permanecendo a dúvida, o Colaborador deve entrar em contato com a área de Tecnologia para maiores explicações e suporte técnico.

9.3. Atualizações

O Sistema Operacional, antivírus e demais sistemas devem permanecer atualizados. O sistema operacional dos equipamentos de Colaboradores deve permanecer com as atualizações automáticas sempre ativas, salvo casos específicos de compatibilidade de sistemas defasados ou testes em ambientes simulados.

9.4. Rastreabilidade

Todas as soluções, sejam elas adquiridas ou desenvolvidas, possuem geração ativa de logs de erros, eventos críticos, entrada e saída de informações relevantes, entre outros eventos. Esse registro pode ser utilizado para restabelecer o estado original de um sistema, para que um administrador conheça o seu comportamento no passado ou até mesmo para análise de auditorias internas e externas.

Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir eventos.

9.5. Cópias de Segurança (Backup)

A importância dos backups na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

Cada departamento/usuário tem acesso a pelo menos uma pasta no servidor e/ou serviço de nuvem de arquivos. Todos os documentos relacionados ao negócio devem ser armazenados nestas pastas. Além disso, cada usuário tem uma pasta individualizada para uso profissional no servidor e/ou serviço de nuvem de arquivos.

Qualquer arquivo armazenado em pastas locais nos computadores não é passível de backup, e por isso o armazenamento nesses locais é de total responsabilidade do usuário.

9.6. Testes de Intrusão

Testes de Intrusão interno e externo pentest nas camadas de rede, aplicações desenvolvidas internamente ou externamente, devem ser realizados no mínimo anualmente. A FIDD estabelece que apenas empresas contratadas por ela podem realizar pentests ou avaliações de segurança em seus sistemas e infraestrutura. Qualquer tentativa de avaliação do ambiente sem conhecimento prévio e autorização por parte da FIDD, acarretará uma investigação para identificação do possível impacto e notificação ao infrator.

9.7. Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente ou sempre que houver mudança significativa na estrutura tecnológica. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

9.8. Segmentação de Rede

As definições de rede estão especificadas no Manual de Infraestrutura, e devem seguir as seguintes regras para garantia da segurança das informações nela trafegadas:

(i) Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;

(ii) Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;
(iii) Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de TI, que fará a análise, aprovação e execução da configuração.

10. DESENVOLVIMENTO SEGURO

A FIDD mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

A FIDD mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

A FIDD adota como prática a segregação física, lógica e administrativa dos ambientes de produção, desenvolvimento, testes/homologação e para alguns casos, pré-produção.

As equipes de desenvolvimento somente terão acesso aos ambientes de produção mediante expressa autorização superior.

Os responsáveis de segurança e as áreas de negócios canalizam todas as diretrizes e normas para o atendimento das necessidades de proteção ao negócio, quais sejam:

- Realizam recomendações de requisitos específicos ao desenvolvimento e manutenção de sistemas com a finalidade de reduzir o grau de exposição a riscos, tais como: possibilidade de ocorrência de fraudes, de vazamento de informações confidenciais, de acessos indevidos, dentre outros.
- Avaliam, por meio de relatórios e métricas, a qualidade dos sistemas desenvolvidos internamente e por empresas subcontratadas no que diz respeito à segurança do código fonte e orienta a fim de que a qualidade deste código seja sempre aprimorada.
- Acompanha os projetos demandados pelas áreas de negócios, de acordo com a metodologia de desenvolvimento e manutenção de sistemas adotada pela FIDD.

Os acessos aos sistemas são realizados através de interfaces de software, que permitem a coleta de logs e trilhas de auditoria. Esses registros garantem a rastreabilidade do sistema.

Todas as alterações de versões dos sistemas em produção ou correções de bugs de programação são realizadas somente com revisão de usuário supervisor nomeado pelo Diretoria de TI.

11. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

As respostas aos incidentes de Segurança da Informação visam assegurar o restabelecimento do nível normal do ambiente tecnológico, após o acontecimento de um sinistro, fornecendo direcionamento para a devida utilização dos recursos e procedimentos fundamentais, garantindo efetividade.

O plano abrange incidentes originados tanto em sistemas de desenvolvimento interno, como em sistemas de empresas prestadoras de serviços.

O plano deve prever o (i) o planejamento, atividade esta que compreende identificar, prever e descrever situações de possíveis sinistras, bem como suas respectivas ações de mitigação, responsáveis, tempos e registros, de forma que, em situações reais, as atividades já estejam previamente mapeadas e as ações já preestabelecidas, (ii) a identificação, esta atividade compreende realizar ações para identificação e registro dos sinistros, (iii) a resposta incidentes de segurança, atividade compreende reações aos possíveis ataques identificados, (iv) vistoria, consiste em ações realizadas após a ocorrência do incidente, como auditorias e análises de vulnerabilidade, (v) o compartilhamento, a FIDD desenvolve iniciativas para o compartilhamento de informações sobre os incidentes ocorridos, abrangendo informações sobre incidentes relevantes e as disponibiliza ao Banco Central do Brasil (BACEN), à Autoridade Nacional de Proteção de Dados (ANPD), outras instituições financeiras e/ou prestadores de serviços contratados, se aplicável.

12. GESTÃO DE CONSEQUÊNCIAS

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios e medidas adiministrativas poderão ser tomadas. Portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar a Diretoria de Riscos ou Equipe de Segurança da Informação.

Controle e Revisão

Registro de Alterações			
Área responsável pela Norma	Riscos e Segurança da Informação		
Versão	**Itens revisados**	**Área Responsável**	**Data**
V1	-	TI	10/03/2020
V2	Alteração de período de revisão obrigatória	TI	30/07/2020
V3	Alteração no tempo de retenção de backups de 7 para 10 dias.	TI	18/11/2020
V4	Revisão da Política	TI	30/07/2021
V5	Atualização no plano de respostas a incidentes, e inclusão da periodicidade dos treinamentos de SI.	Segurança da Informação	28/07/2022
	Atualização anual	Segurança da Informação	30/08/2024
V8	Alteração de norma regulatória	Segurança da Informação	26/12/2024
Classificação da Informação			**Pública**

Revisão e Alterações		
Etapa	**Responsável**	**Área**
Elaboração/Atualização	Anderson Fossa, Bruno Warmling e Alexandre Noboru Chára	Segurança da Informação e Riscos
Revisão	Controles Internos e Compliance	Controles Internos e Compliance
Aprovação	Diretoria	Diretoria Executiva
Vigência	1 (um) ano após a Data da Última Aprovação	